SPYWOLF

Security Audit Report

Completed on

June 30, 2022

MADE IN USA 🇺🇸

OVERVIEW

This audit has been prepared for **iDot Finance** to review the main aspects of the project to help investors make make an informative decision during their research process.

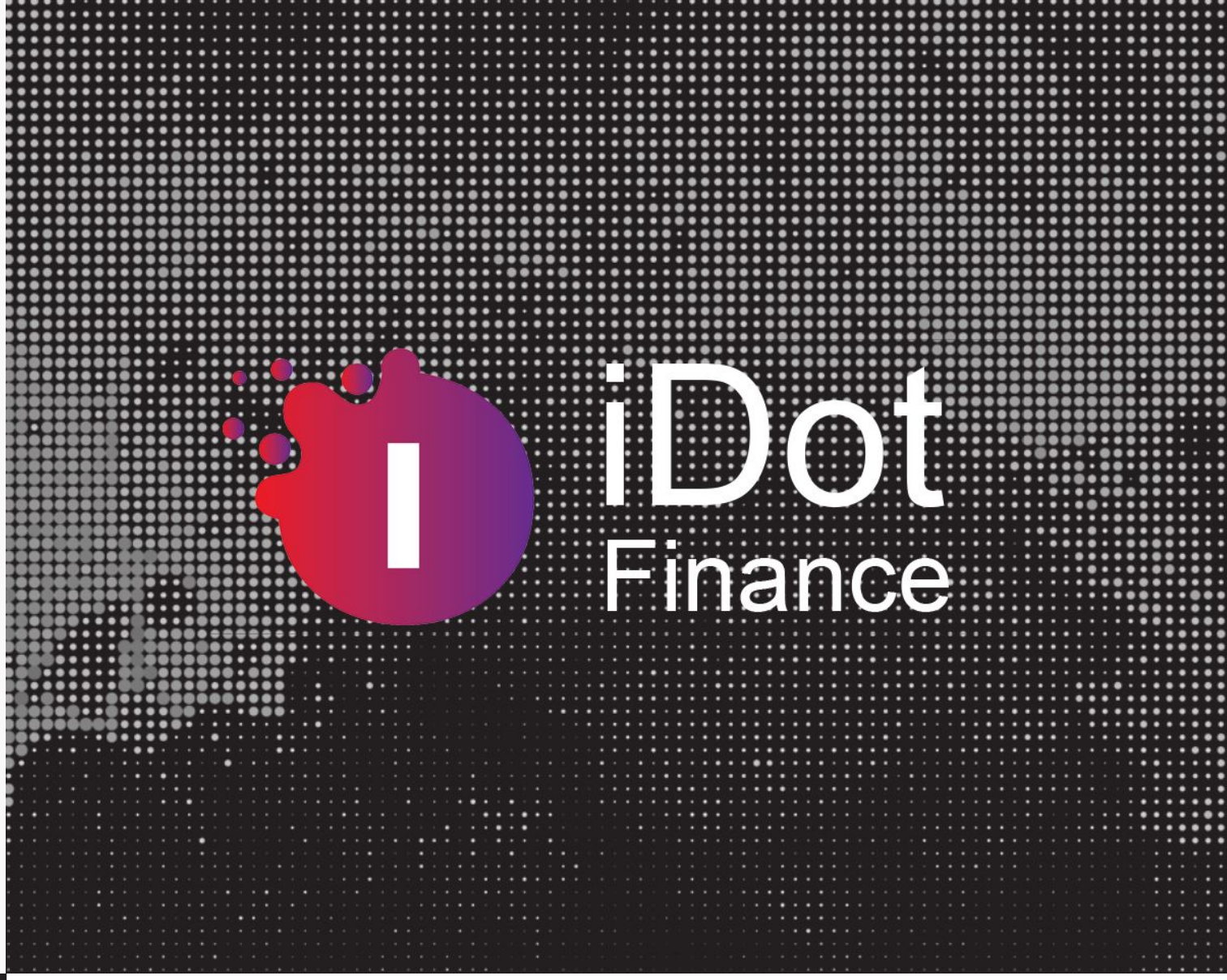
You will find a a summarized review of the following key points:

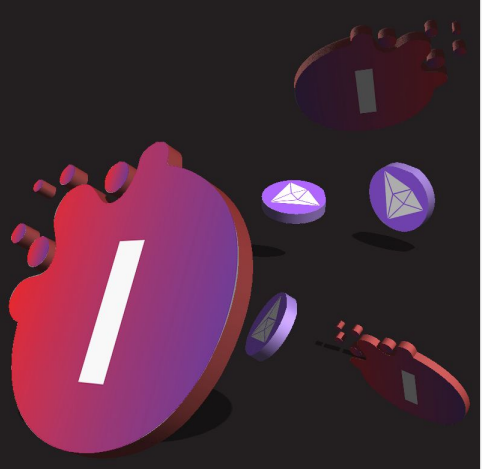
- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS





PROJECT DESCRIPTION

According to their whitepaper:

iDot Finance combine Halving Process, Tax Reflection, Tax Referral, Staking process on Proof of Hold combined with Auto-Compounding into your wallet.

iDot Protocol will be known as Proof of Hold & Hold to Earn.

Release Date: Presale starts on July, 2022

Category: Rebase / Hold to earn

CONTRACT INFO

Token Name	Symbol
iDot Finance	IDOT

Contract Address
0x9650Fd508E47c0f8787237f06E293fc299332603

Network	Language
Binance Smart Chain	Solidity

Deployment Date	Verified?
June 24, 2022	Yes

Total Supply	Status
1,450,000	Not launched

TAXES

Buy Tax
10.6%

Sell Tax
14.6%

*Taxes cannot be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

CURRENT STATS

(As of June 30, 2022)

Liquidity

Not added yet

Burn

No burnt tokens

Status:

Not Launched!

MaxTxAmount

No limit

DEX:

PancakeSwap

LP Address(es)

Liquidity not added yet

TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	1450000 IDOT
Median Transfer Amount	1450000 IDOT
Average Transfer Amount	1450000 IDOT
First transfer date	2022-06-24
Last transfer date	2022-06-24
Days token transferred	1

SMART CONTRACT STATS

Calls Count	1
External calls	1
Internal calls	0
Transactions count	1
Uniq Callers	1
Days contract called	1
Last transaction time	2022-06-24 16:11:23 UTC
Created	2022-06-24 16:11:23 UTC
Create TX	0x5e3ccefb6a82e695e90cd6e5416d333deeab9c8bac3d83cfd6ca119fb3ebefaa
Creator	0xd784d85662cc9e48fc43dc9dee1371cb967adc56

FEATURED WALLETS

Owner address	0xd784d85662cc9e48fc43dc9dee1371cb967adc56
Automatic LP fund	Same as owner
Obsidium capital fund	0xc005ef0ebf220e3824a5739f5085885dc8a00115
Rebase pool fund	0xc20a0221ce396c26989b8bd5c6ed91e8b6691213
Sell fee fund	0x88af6d47b53a0acb54fccb160cfc7eb587fdbf1d
LP address	**Liquidity not added yet**

TOP 3 UNLOCKED WALLETS

1

100% Same as owner

⚠️Tokens are not distributed yet

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ Medium Risk

Owner can blacklist only contracts.
If liquidity pair is blacklisted, this will lead to inability to trade.

```
function setBotBlacklist(address _botAddress, bool _flag) external authorized {
    require(isContract(_botAddress), "Only contract address, not allowed externally owned account");
    blacklist[_botAddress] = _flag;
}
```

Owner can add referrals to address.

```
function addMember(address uplineAddress, address downlineAddress) external onlyOwner{
    downlineLookupUpline[downlineAddress] = uplineAddress;
}
```

Function should be declared as internal, because anyone can change the values.

```
function addReferralFee(address receiver, uint256 amount) public {
    referralTotalFeeReceived[receiver] += amount;
}
```

- Recommendation:
  - Considered as good wallet restrictions practice is that liquidity pair is always excluded from such practices.

⚠ Low Risk

Owner can turn on and off rebase.

```
function setAutoRebase(bool _flag) external authorized {
    if (_flag) {
        _autoRebase = _flag;
        _lastRebasedTime = block.timestamp;
    } else {
        _autoRebase = _flag;
    }
}

function shouldRebase() internal view returns (bool) {
    return
        _autoRebase &&
        (_totalSupply < MAX_SUPPLY) &&
        msg.sender != pair  &&
        !inSwap &&
        block.timestamp >= (_lastRebasedTime + 60 minutes);
}
```

Informational

This is rebase token with changing supply up to 14,500,000.
Current supply is 1,450,000.

```
uint256 private constant INITIAL_FRAGMENTS_SUPPLY = 1450000 * 10**DECIMALS;
uint256 private constant MAX_SUPPLY = 14500000 * 10**DECIMALS;

function shouldRebase() internal view returns (bool) {
    return
        _autoRebase &&
        (_totalSupply < MAX_SUPPLY) &&
        msg.sender != pair  &&
        !inSwap &&
        block.timestamp >= (_lastRebasedTime + 60 minutes);
}
```

Owner can withdraw accumulated bnb tokens from the contract.

```
function clearStuckBalance(uint256 amountPercentage) external authorized {
    uint256 amountBNB = address(this).balance;
    payable(obsidiumCapitalFund).transfer(amountBNB * amountPercentage / 100);
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

iDot Finance

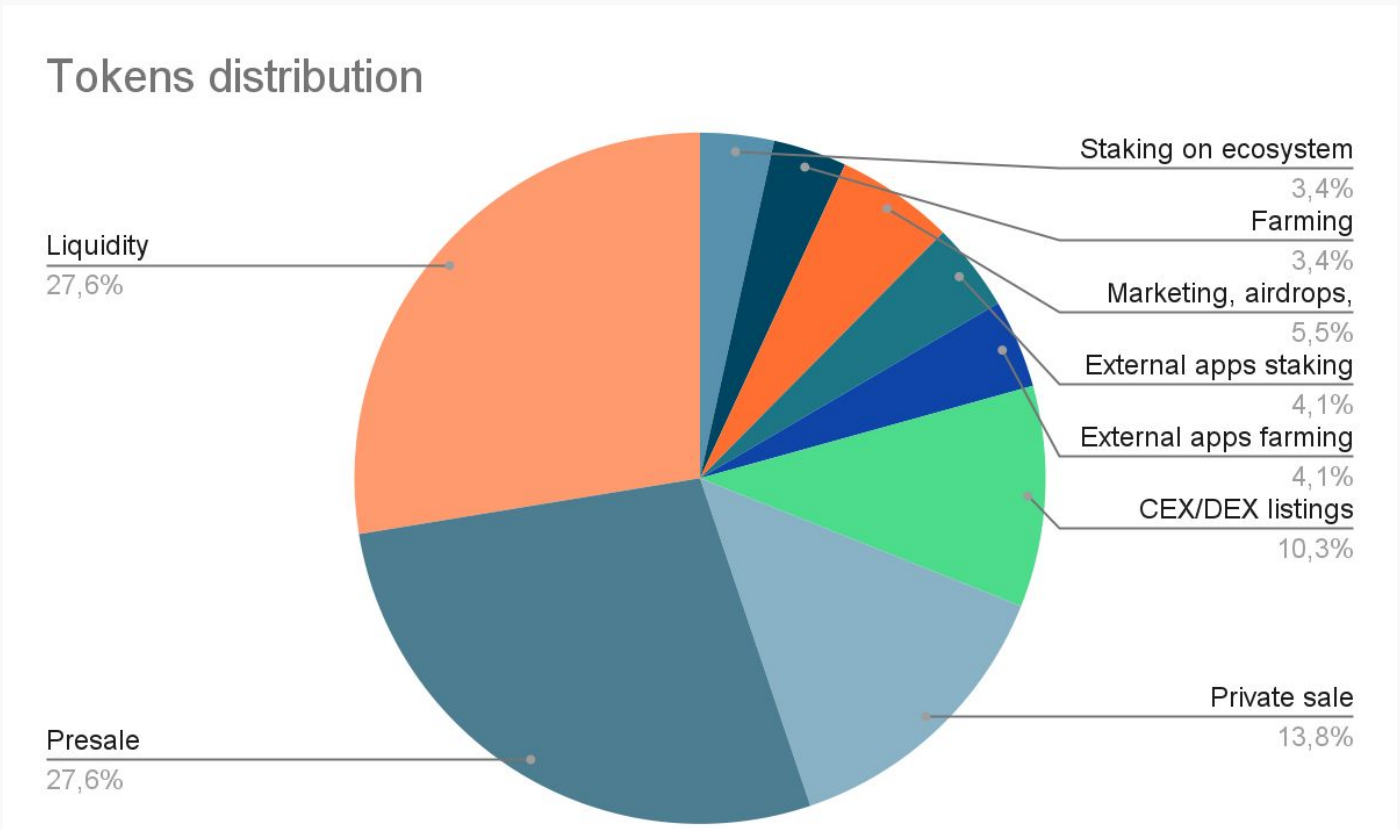
GOOD PRACTICES FOUND

- ✔ The owner cannot mint new tokens after deployment
- ✔ The owner cannot stop or pause the contract
- ✔ The owner can set a transaction limit, but can’t lower it than 1% of total supply
- ✔ The smart contract utilizes "SafeMath" to prevent overflows

TOKENOMICS

The following tokens distribution information is based on the project's whitepaper and/or website.

- 27,6% - Presale
- 13.6% - Private sale
- 27.6% - Liquidity
- 10% - CEX/DEX listings
- 4.1% - Farming on external apps
- 3.4% - Staking on ecosystem apps
- 3.4% - Farming
- 5.5% - Marketing, airdrops, bounty
- 4.1% - Staking on external apps



THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

⚠️ No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.

WEBSITE

Website URL
https://www.idot.finance/

Domain Registry
https://www.namecheap.com/

Domain Expiration
Expires on 2023-06-07

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

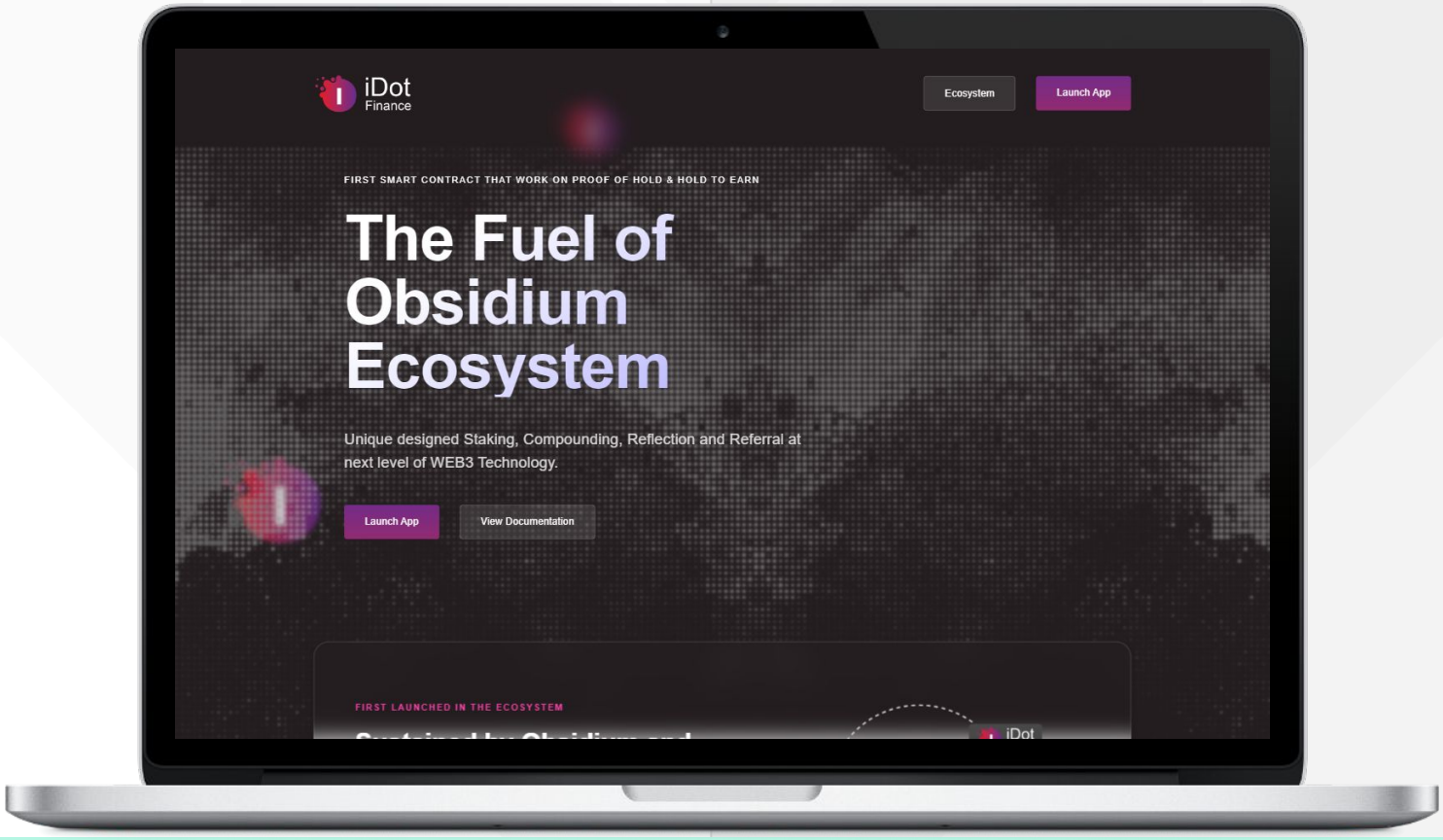
Design
Nice color scheme and overall layout.

Content
The information helps new investors understand what the product does right away. No grammar errors found.

Whitepaper
Well written, explanatory.

Roadmap
Partial, goals set for Q3.

Mobile-friendly?
Yes



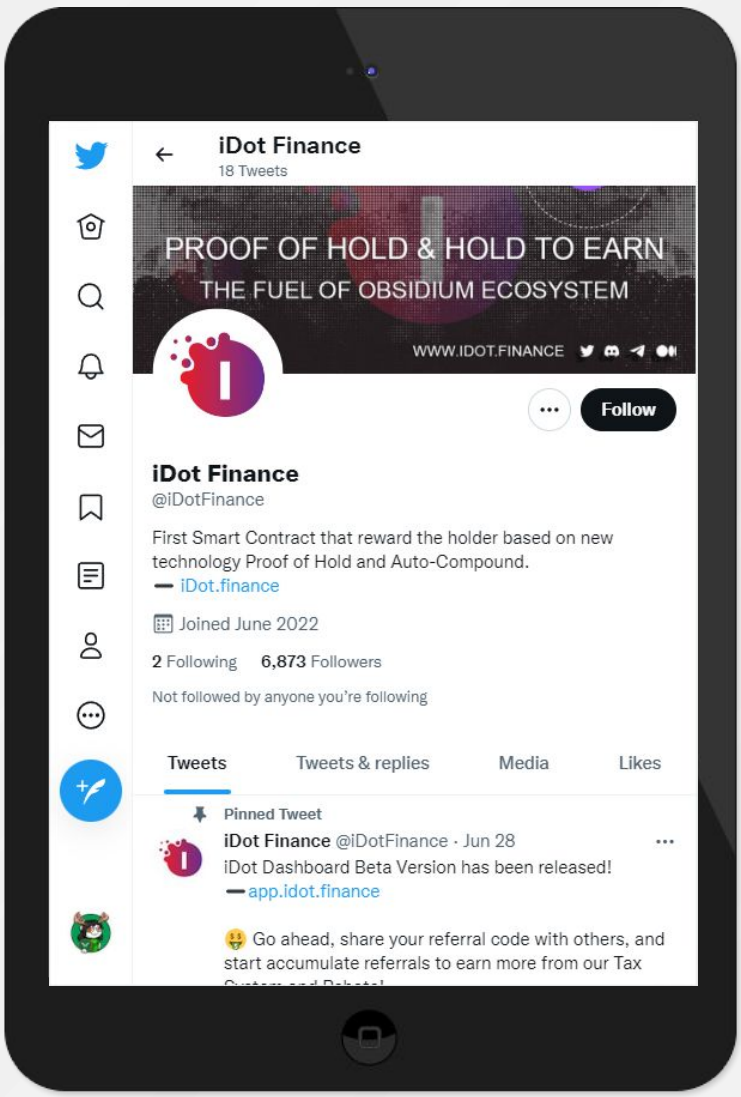
idot.finance

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media presence is relatively new (few days old). The mods are active, but there are few organic interaction, and bot-like behaviors were detected ⚠️.



Twitter

@iDotFinance

- 6,873 followers
- Recently active - 18 tweets, last one June 28
- Few active followers - doesn't correspond to followers number ⚠️

Discord

https://discord.com/invite/obsidiumcc

- 660 members
- Active mods/team
- Few interactions, bot-like in majority ⚠️

Telegram

@iDotFinance

- 919 members
- Active mods/team
- Organic interactions

Medium

Medium link here

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 150 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

SPYWOLF.NETWORK

@SPYWOLFNETWORK

@SPYWOLFOFFICIAL

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.